



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|-------------|----------------------|-----------------------|------------------|
| 09/648,211 | 08/25/2000 | John S. Flowers | HVWD-01001US0-MEM/SBS | 5311 |
| 758 | 7590 | 06/08/2004 | EXAMINER | |
| FENWICK & WEST LLP SILICON VALLEY CENTER 801 CALIFORNIA STREET MOUNTAIN VIEW, CA 94041 | | | MOORTHY, ARAVIND K | |
| | | ART UNIT | PAPER NUMBER | 10 |
| | | 2131 | | |

DATE MAILED: 06/08/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

| | | |
|------------------------------|------------------------|---------------------|
| Office Action Summary | Application No. | Applicant(s) |
| | 09/648,211 | FLOWERS ET AL. |
| | Examiner | Art Unit |
| | Aravind K Moorthy | 2131 |

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 10 March 2004.
 2a) This action is FINAL. 2b) This action is non-final.
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-45 is/are pending in the application.
 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
 5) Claim(s) _____ is/are allowed.
 6) Claim(s) 1-28 and 30-45 is/are rejected.
 7) Claim(s) 29 is/are objected to.
 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
 10) The drawing(s) filed on 25 August 2000 is/are: a) accepted or b) objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____ | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Claims 1-45 are pending in the application.
2. Claims 1-28 and 30-45 have been rejected.
3. Claim 29 have been objected to.

Response to Arguments

4. Applicant's arguments with respect to claims 1-45 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

5. **Claims 1-5, 8-20, 23-28, 30, 33, 34 and 39-45 are rejected under 35 U.S.C. 102(e) as being anticipated by Shostack et al U.S. Patent No. 6,298,445B1.**

Art Unit: 2131

As to claims 1, 13 and 39, Shostack et al discloses identifying an operating system of a remote host [column 7, lines 20-30]. Shostack et al suggests that it includes a version and a patch level of the operating system. Shostack et al suggests identifying a service of the remote host including a version and a patch level of the service. Shostack et al discloses identifying a vulnerability of the network based on information obtained from the steps of identifying an operating system and identifying a service [column 5 line 55 to column 6 line 35].

As to claims 2, 12, 17 and 45, Shostack et al discloses that the step of identifying an operating system includes sending a first set of packets to the remote host and receiving a second set of packets from the remote host in response to the first set of packets. Shostack et al discloses that the step of identifying a service includes sending a third set of packets to the remote host and receiving a fourth set of packets from the remote host in response to the third set of packets. Shostack et al discloses that the information contained in the third set of packets is based on information received in the second set of packets. Shostack et al discloses that the step of identifying a vulnerability includes comparing information contained in the second set of packets and the fourth set of packets to preexisting information in a database [column 9 line 56 to column 10 line 9].

As to claim 3, Shostack et al suggests that the step of identifying an operating system includes sending three sets of packets to the remote host and receiving three respective sets of responsive packets from the remote host [column 9 line 56 to column 10 line 9].

As to claim 4, Shostack et al suggests nonintrusively and reliably identifying an operating system of a remote host including identifying a version of the operating system. Shostack et al

Art Unit: 2131

discloses nonintrusively and reliably identifying a service of the remote host including identifying a version of the service [column 12, lines 14-26].

As to claim 5, Shostack et al discloses identifying a vulnerability of the network [column 12, lines 41-57].

As to claim 8, Shostack et al discloses identifying security policy violations on the network [column 13, lines 37-44].

As to claim 9, Shostack et al discloses the step of identifying an operating system further includes identifying a patch level of the operating system. Shostack et al discloses the step of identifying a service further includes identifying a patch level of the service, as discussed above.

As to claim 10, Shostack et al discloses sending a selected packet to the remote host. Shostack et al discloses receiving from the remote host a reflexive responsive packet [column 7, lines 11-19].

As to claim 11, Shostack et al discloses sending a plurality of selected packets to the remote host. Shostack et al discloses receiving from the remote host a plurality of reflexive responsive packets [column 7, lines 11-19].

As to claim 14, Shostack et al discloses that the step of identifying a vulnerability includes using information obtained from the steps of identifying an operating system and identifying a service to identify the vulnerability, as discussed above.

As to claim 15, Shostack et al discloses that the step of identifying an operating system further includes identifying a patch level of the operating system, as discussed above. Shostack et al discloses that the step of identifying a service includes identifying a patch level of the service, as discussed above.

As to claim 16, Shostack et al discloses sending a selected packet to the remote host. Shostack et al discloses receiving from the remote host a reflexive responsive packet, as discussed above.

As to claim 18, Shostack et al suggests that the information contained in the third set of packets is based on information received in the second set of packets. Shostack et al suggests that the information contained in the fifth set of packets is based on information received in the fourth set of packets [column 7, lines 37-65].

As to claim 19, Shostack et al discloses sending a set of selected packets to a host on the network. Shostack et al discloses receiving from the remote host a set of reflexive responsive packets. Shostack et al discloses identifying conditions of the remote host by using information received in the reflexive responsive packets. Shostack et al discloses that the conditions include an operating system of the host, and a service of the host [column 7, lines 37-65].

As to claim 20, Shostack et al discloses that the conditions further include a vulnerability of the host, as discussed above.

As to claim 23, Shostack et al discloses that identifying an operating system includes identifying a version, as discussed above. Shostack et al discloses that identifying a service includes identifying a version, as discussed above.

As to claim 24, Shostack et al discloses that identifying an operating system includes identifying a version and a patch level, as discussed above. Shostack et al discloses that identifying a service includes identifying a version and a patch level, as discussed above.

As to claim 25, Shostack et al discloses that the step of sending a yet of selected packets to a host on the network includes sending a plurality of sets of packets to the host. Shostack et al

discloses that the step of receiving from the remote host a set of reflexive responsive packets includes receiving a like plurality of sets of reflexive responsive packets [column 7, lines 37-65].

As to claims 26, 40, 41 and 44, Shostack et al discloses sending a first set of selected packets to a host on the network. Shostack et al discloses receiving a second set of packets from the remote host in response to the first set of packets. Shostack et al discloses sending a third set of selected packets to a host on the network. Shostack et al discloses that the information contained in the third set of packets is based on information contained in the second set of packets. Shostack et al discloses receiving a fourth set of packets from the remote host in response to the third set of packets. Shostack et al discloses sending a fifth set of selected packets to a host on the network. Shostack et al discloses that the information contained in the fifth set of packets is based on information contained in the fourth set of packets. Shostack et al discloses receiving a sixth set of packets from the remote host in response to the fifth set of packets. Shostack et al discloses based on information contained in the second, fourth, and sixth set of packets, identifying an operating system of a host on the network, including a version and a patch level [column 7, lines 37-65].

As to claim 27, Shostack et al discloses sending a seventh set of selected packets to a host on the network. Shostack et al discloses receiving an eighth set of packets from the remote host in response to the seventh set of packets. Shostack et al discloses sending a ninth set of selected packets to a host on the network. Shostack et al discloses receiving a tenth set of packets from the remote host in response to the ninth set of packets. Shostack et al discloses that based on information contained in the eight and tenth sets of packets, identifying a service of a host on the network, including a version and a patch level [column 7, lines 37-65].

As to claim 28, Shostack et al discloses that based on information contained in at least the tenth sequence, identifying a vulnerability [column 7, lines 37-65].

As to claim 30, Shostack et al discloses sending a plurality of packets to a network, as discussed above. Shostack et al discloses receiving a responsive plurality of packets from the network, as discussed above. Shostack et al discloses comparing information in the responsive packets to information stored in a database. Shostack et al discloses that based on the comparison, identifying a plurality of network conditions, including a vulnerability of the network [column 8, lines 7-40].

As to claim 33, Shostack et al discloses sending packets to a network, as discussed above. Shostack et al discloses receiving responsive packets from the network, as discussed above. Shostack et al discloses comparing information in the responsive packets to information stored in a database, as discussed above. Shostack et al discloses that based on the comparison, inferring an unknown vulnerability [column 7, lines 32-53].

As to claim 34, Shostack et al discloses sending packets to a network, as discussed above. Shostack et al discloses receiving responsive packets from the network, as discussed above. Shostack et al discloses comparing information in the responsive packets to information stored in a database, as discussed above. Shostack et al discloses that based on the comparison, identifying a security policy violation [column 6, lines 37-65].

As to claim 42, Shostack et al discloses receiving a set of selected packets from remote equipment, as discussed above. Shostack et al discloses automatically sending a second set of packets to the remote equipment, which packets include information that enables the remote equipment to identify a vulnerability on the network, as discussed above

As to claim 43, Shostack et al suggests receiving a first set of packets from remote equipment. Shostack et al suggests automatically sending a second set of packets to the remote equipment. Shostack et al suggests receiving a third set of packets from the remote equipment. Shostack et al suggests automatically sending a fourth set of packets to the remote equipment. Shostack et al suggests receiving a fifth set of packets from the remote equipment. Shostack et al suggests automatically sending a sixth set of packets from the remote equipment. Shostack et al suggests receiving a seventh set of packets from the remote equipment. Shostack et al suggests automatically sending an eighth set of packets from the remote equipment. Shostack et al suggests receiving a ninth set of packets from the remote equipment. Shostack et al suggests automatically sending a tenth set of packets from the remote equipment. Shostack et al suggests that the second, fourth, and sixth sets of packets include information that enables the remote equipment to identify an operating system on the network, including a version and a patch level. Shostack et al suggests that the eighth and tenth sets of packets include information that enables the remote equipment to identify a service, including a version and a patch level [column 5, lines 6-51].

6. Claims 31, 35, 36 and 38 are rejected under 35 U.S.C. 102(e) as being anticipated by Hill et al U.S. Patent No. 6,088,804.

As to claim 31, Hill et al discloses sending packets to a network [column 5, lines 26-45]. Hill et al discloses receiving responsive packets from the network [column 5, lines 46-65]. Hill et al discloses comparing information in the responsive packets to information stored in a database [column 6, lines 9-22]. Hill discloses based on the comparison, identifying a Trojan application on the network [column 5, lines 46-65].

As to claim 35, Hill et al discloses a database including a set of reflex signatures [column 5, lines 46-65]. Hill discloses a packet generator [column 6, lines 9-22]. Hill et al discloses a comparison unit in communication with the packet generator and the database [column 6, lines 9-22]. Hill et al discloses that the packet generator is designed to generate and transmit a plurality of test packets to the network [column 5, lines 8-15]. Hill et al discloses that the comparison unit is designed to receive responsive packets from the network and to compare responsive packet information with the reflex signatures [column 5, lines 46-65].

As to claim 36, Hill et al discloses that the comparison unit is further designed to identify a vulnerability in the network based on its comparison of packet information with reflex signatures [column 6, lines 32-60].

As to claim 38, Hill et al discloses that the comparison unit is designed to provide information to the packet generator, and wherein the packet generator is designed to use the information to selectively generate packets [column 5, lines 6-65].

7. Claim 32 is rejected under 35 U.S.C. 102(e) as being anticipated by Diersch et al U.S. Patent No. 6,101,606.

As to claim 32, Diersch et al discloses sending packets to a network [column 5, lines 11-65]. Diersch et al discloses receiving responsive packets from the network [column 5, lines 11-65]. Diersch et al discloses comparing information in the responsive packets to information stored in a database [column 5, lines 11-65]. Diersch et al discloses that based on the comparison, identifying unauthorized software use on the network [column 5, lines 11-65].

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

8. Claims 6 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shostack et al U.S. Patent No. 6,298,445B1 as applied to claim 1 above, and further in view of Drake U.S. Patent No. 6,006,328.

As to claims 6 and 22, Shostack et al does not teach identifying a Trojan application on the host.

Drake teaches identifying a Trojan application on the host [column 1 line 56 to column 2 line 2].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Shostack et al so that when the operating system is being identified that a Trojan application on the host was also identified.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Shostack et al by the teaching of Drake because it prevents eavesdropping, prevents disassembly and examination, detects tampering, prevents execution-tracing and ensures authenticity [column 5, lines 3-14].

9. Claims 7 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shostack et al U.S. Patent No. 6,298,445B1 as applied to claim 1 above, and further in view of Hornbuckle U.S. Patent No. 5,388,211.

As to claims 7 and 21, Shostack et al does not teach identifying unauthorized software use on the host.

Hornbuckle teaches identifying unauthorized software use on the host [column 3, lines 6-63].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Shostack et al so that when the operating system is being identified that unauthorized software use was also identified on the host.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Shostack et al by the teaching of Hornbuckle because it prevents theft, copying, vandalism or modification [column 3, lines 6-15].

10. Claim 37 is rejected under 35 U.S.C. 103(a) as being unpatentable over Hill et al U.S. Patent No. 6,088,804 as applied to claim 35 above, and further in view of Shostack et al U.S. Patent No. 6,298,445B1.

As to claim 37, Hill et al does not teach that the comparison unit is further designed to identify an operating system type, version, and patch level and a service type, version, and patch level of a host on the network.

Shostack et al teaches a comparison unit that is designed to identify an operating system type, version, and patch level and a service type, version, and patch level of a host on the network, as discussed above.

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Hill et al so that the comparison unit would have

identified an operating system type, version, and patch level and a service type, version, and patch level of a host on the network.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Hill et al by the teaching of Shostack et al because the examiner asserts that certain versions of some operating system are known to have known vulnerabilities as well as service types and patch levels. Therefore, it would be necessary to check these elements on a host to prevent exploitations on these known vulnerabilities.

Claim Objections

11. Claim 29 is objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

As to claim 29, prior art does not teach a first set of packets that includes: a SYN Packet with false flag in the TCP option header; a Fragmented UDP packet with malformed header (any header inconsistency is sufficient), where the packet is 8K in size; a FIN Packets of a selected variable size or a FIN packet without the ACK or SYN flag properly set; and a generic, well-formed ICMP ECHO request packet. Prior art does not teach a third set of packets includes: a generic well-formed TCP Header set to 1024 bytes in size; a packet requesting an ICMP Timestamp; a packet with min/max segment size set to a selected variable value; and a UDP packet with the fragment bit set. Prior art does not teach a fifth set of packets includes: a TCP Packet with the header and options set incorrectly; a well-formed ICN11P Packet; a Fragmented TCP or UDP packet; a packet with an empty TCP window or a window set to zero; a generic TCP Packet with 8K of random data; and a SYN Packet with ACK and RST flags set.

Conclusion

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K Moorthy whose telephone number is 703-305-1373. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Aravind K Moorthy
May 27, 2004


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100